scripted

Volume 14, Issue 2, December 2017

# Quantified Self, Freedom, and the GDPR

*Minke D. Reijneveld**



DOI: 10.2966/scrip.140217.285

**Abstract**

The General Data Protection Regulation (GDPR) will be applied from May 2018. One of the many new societal developments it has to deal with is the Quantified Self (QS). This concerns data that are collected about a person by apps that aim to improve his or her life. This article answers the question to what extent the tools and assumptions that underlie the creation of QS influence an individual's freedom and to what extent the GDPR can contribute to the protection of this freedom.

The article finds that QS can restrict an individual's internal and external freedom. It suggests that everybody should meet a certain standard or group norm, which influences the choices individuals make. This is an internal restriction of freedom, which is largely unknown. A more familiar problem is the external restriction of freedom. This happens when data are analysed by the QS app or by third parties. They can make assumptions about a person on the basis of these data, which influences the possible options for an individual.

The GDPR does protect certain elements of external freedom better than

the EDPD. This mainly has to do with the rules related to data about health, and more stringent rules in general. The GDPR does not protect the internal aspect of freedom, although the possible risks of this internal restriction can be very serious.

**Keywords**
GDPR; privacy; Quantified Self; freedom; autonomy

* Student Legal Research Master, Law, Utrecht University, Utrecht, the Netherlands, m.d.reijneveld@uu.nl

## 1 Introduction

The General Data Protection Regulation (GDPR) is a new European Regulation that will be applied from 2018.[1] The GDPR has to deal with many technologies that have been created since its predecessor, the European Data Protection Directive (EDPD),[2] was created in 1995. The GDPR is "designed to harmonize data privacy laws across Europe, to protect and empower all EU citizens data privacy and to reshape the way organizations across the region approach data privacy."[3] The GDPR will replace the EDPD, once it becomes enforceable.[4] Unlike the EDPD, this regulation will be directly applicable in all Member States. Directives, on the other hand, are addressed at Member States and not legally binding for individuals. The European Parliament and Council have decided on a regulation instead of a directive because they observed that the EDPD has not lead to sufficient harmonisation of data protection laws across Member States.[5] Moreover, the Commission wants to promote a single market without obstacles for the free movement of data, which can be reached by enhanced unification of law.[6] This is explicitly mentioned in recital 10 of the GDPR which states that the "level of protection of rights and freedoms of natural persons […] should be

* The author would like to thank her supervisor Dr. M. van der Linden-Smith for all the valuable feedback, support and interesting conversations. Additionally, the author would like to thank the anonymous reviewers for their feedback.

1 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L 119/1 (hereinafter 'GDPR').

2 Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L 281 (hereinafter 'EDPD').

3 See "GDPR Portal: Site Overview" available at http://www.eugdpr.org/ (accessed 5 December 2017).

4 This will be on 25 May 2018.

5 GDPR, rec. 7.

6 *Ibid*., rec. 11.

equivalent in all Member States."[7]

The current EDPD and the future GDPR do not stand on their own, but are part of a legal system of privacy protection that is applicable to all Member States of the European Union. This means there are more rules applicable to privacy protection than the EDPD or GDPR. Privacy is actually one of the oldest human rights in Europe, and is protected by many human rights treaties.[8] As a human right, it is protected in article 8 of the European Convention on Human Rights, which protects the right to private life. Although the European Union is not a party to this convention, and will not become a part of it in the near future,[9] all EU Member States are parties.[10] The same holds true for the Universal Declaration of Human Rights, which protects individuals against arbitrary interferences with their privacy in article 12. Furthermore, the Charter of Fundamental Rights of the European Union recognises the right to privacy in article 7, and a right to data protection in article 8. Moreover, the right to personal data is also recognised in article 16 of the Treaty on the Functioning of the European Union (TFEU).[11] These rights are linked to privacy, and are not discussed separately in this article. Finally, privacy is also protected under article 17 of the International Covenant on Civil and Political Rights.[12] The EDPD was established on top of all these rules in the mid-1990s, to provide a regulatory

---

7 *Ibid*., rec. 10.

8 Francesca Bignami, "Privacy and Law Enforcement in the European Union: The Data Retention Directive" (2007) 8(1) *Chicago Journal of International Law* 233 – 255, p. 233.

9 According to the EU's Treaty of Lisbon, the EU is required to accede the ECHR (Consolidated Version of the Treaty on the Functioning of the European Union (TFEU) [2010] OJ C 83/47 art. 6). However, on 18 December 2014, the Court of Justice issued a negative opinion on the accession of the EU to the ECHR (Opinion 2/13 [2014]).

10 *Supra* n. 8, pp. 241-242.

11 TFEU *supra* n. 9, art. 16.

12 International Covenant on Civil and Political Rights Adopted and opened for signature, ratification and accession by General Assembly resolution 2200A (XXI) of 16 December 1966 entry into force 23 March 1976, in accordance with Article 49.

framework to guarantee secure and free movement of personal data across the national borders of the EU Member States. The EDPD focuses on the protection of individual rights,[13] and also explicitly refers to the legal framework given in the human rights treaties mentioned above.[14] This is the same for the GDPR, which is based on article 16 of the TFEU.[15] The main aim of the GDPR is "to enhance data protection rights of individuals and to improve business opportunities by facilitating the free flow of personal data in the digital single market."[16]

The key principles of data privacy and protection are the same for the EDPD and the GDPR,[17] but many substantive provisions are different in the GDPR. Furthermore, the GDPR is far more extensive than the EDPD. Throughout this article, references to the EDPD and GDPR will be made in order to highlight potential flaws with respect to Quantified Self (QS) and to identify possible advantages of the GDPR. This will show what new challenges QS poses to the EDPD and whether those new challenges are better addressed by the new GDPR.

Since the creation of the EDPD in 1995, many new technological developments have taken place. Think for example about the creation of Google

---

13 Francesca Bignami, "Transgovernmental Networks vs. Democracy: The Case of the European Information Privacy Network" (2005) 26(565) *The Michigan Journal of International Law* 807-870, pp. 813-819.

14 EDPD, rec. 10.

15 Gerrit Hornung, "A General Data Protection Regulation for Europe? Light and Shade in the Commission's Draft of 25 January 2012" (2012) 9(1) *SCRIPTed* 64-81.

16 Interinstitutional File 2012/0011 (COD), Presidency to the Council, 11 June 2015, 9565/15, Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) - Preparation of a general approach.

17 See "GDPR Key Changes" available at http://www.eugdpr.org/key-changes.html (accessed 5 December 2017).

(1998),[18] and Facebook (2004),[19] and the invention of Wi-Fi (1999).[20] One of the societal trends that has come up with the creation of new technologies is QS, on which this article focuses. This is interesting because there is a tension between the GDPR and QS. The GDPR is about protecting privacy by "imposing constraints on collection and dissemination of personally identifiable information",[21] while QS is generally about collecting and analysing as much personal data about an individual as possible. These two very different goals seem inherently conflicting. Not much has been written yet about the GDPR in connection with QS,[22] and especially not about the link with freedom. This article aims to contribute to the debate by distinguishing between internal and external freedom, and analysing whether and how these are protected by the GDPR. Section three will go into more detail concerning the definitions of privacy, autonomy and freedom.

First, the term 'Quantified Self' (QS) is explored further. Then, in section three, the meaning of freedom, autonomy and privacy are discussed. Section four discusses the elements of the GDPR that are of specific importance for QS. Section five discusses how QS affects freedom and whether or not the GDPR can help to protect that freedom. Finally, section six concludes that the GDPR has some positive influences on the parts of QS that affect our freedom. However, this is

---

18 Google was founded on 4 September 1998 by Larry Page and Sergey Brin.

19 Facebook was launched on 4 February 2004 by Mark Zuckerberg and Eduardo Saverin.

20 In 1999, six companies together created the Wireless Ethernet Compatibility Alliance. They decided to call their body Wi-Fi, and thus Wi-Fi was created in 1999. For more information, see: The Economist, "A brief history of Wi-Fi" (2004) *The Economist, Technology Quarterly Q2*, available at http://www.economist.com/node/2724397 (accessed 5 December 2017).

21 Dominik Leibenger, Frederik Möllers, Anna Petrlic, Ronald Petrlic and Christoph Sorge, "Privacy Challenges in the Quantified Self Movement – An EU Perspective" (2016) 4 *Proceedings on Privacy Enhancing Technologies* 315-334.

22 *Ibid*.

limited to external freedom. The GDPR does not appear to touch upon internal freedom.

## 2 Quantified Self

Quantified Self as an often-used term to describe a societal movement, was introduced in 2007 by Kelly and Wolf.[23] They define QS as "self-knowledge through numbers".[24] Self-tracking, life logging, and QS are synonyms. These terms refer to "the practice of gathering data about oneself on a regular basis and then recording and analysing the data to produce statistics and other data".[25] Normally, the use of QS is aimed at improving a lifestyle (such as achieving a very healthy lifestyle) or achieving a certain goal (e.g. running a marathon or losing a certain amount of weight).[26] QS as a movement is about increasing individual freedom by improving certain aspects of life.

QS can be related to *the situation* in which people record data about themselves.[27] It can also concern *the individual* that is engaged in the self-tracking of any information.[28] Moreover, it can concern *the data* that are collected by persons about themselves. These data have an important role in the formation of

---

23 Gary Wolf, "What is the Quantified Self?" [2011] available at http://quantifiedself.com/2011/03/what-is-the-quantified-self/ (accessed 5 December 2017). The Quantified Self Company provides users a community and it organises amongst other things meetings, conferences, forums, web content, and a guide.

24 See "Quantified Self: self knowledge through numbers" available at http://quantifiedself.com (accessed 5 December 2017).

25 Deborah Lupton, "Understanding the Human Machine" (2013) 32(4) *IEEE Technology and Society Magazine* 25-30, p. 25.

26 Mario Ballano Barcena, Candid Wueest, and Hon Lau, "How Safe is Your Quantified Self?" (2014) *Technical Report Symantec* 1-38.

27 Margreet Riphagen et al., "Learning Tomorrow: Visualising Student and Staff's Daily Activities and Reflect on it" (2013) *ICERI 2013 conference proceedings*, p. 1.

28 Melanie Swan, "The Quantified Self: Fundamental Disruption in Big Data Science and Biological Discovery" (2013) 1(2) *Big Data* 85-99, p. 85.

knowledge about oneself.[29] The focus of this article is on the technologies that are used in the context of the QS movement. Most of these are related to self-tracking. QS is seen as the umbrella concept that includes different technologies. For this article, I will only use QS as referring to *the data* that people collect about themselves by using applications that help to improve his or her life. QS is the overlapping term and includes the use of many technologies.

The data in a QS-device can either be collected automatically or must be fed by the user. Automatic collection is done for example by a footstep-tracker, that counts and collects every step you take, whereas when you keep track of your diet, you have to manually enter what you eat. QS uses various methods to 'quantify' a person's approach to life, health, mood, locations, personal goals (such as sport) and more.[30] More precisely, it can be used for the self-tracking of "any kind of biological, physical, behavioral, or environmental information".[31] Both the automatic collection and the manual data entry usually happen by devices such as smartphones, because they can track a person's movements, pulse or (running) speed, and are always at hand.[32] Popular apps are for example MoodPanda,[33] RunKeeper,[34] and Lose It.[35]

The idea that persons collect data about themselves is not new. The notion of a societal QS movement can be seen rather as a new set of terminology (QS, self-tracking, etc.) for a habit that has been common for a long time: tracking and

---

29 Minna Ruckenstein and Mika Pantzar, "Beyond the Quantified Self: Thematic Exploration of a Dataistic Paradigm" (2015) 19(3) N*ew Media & Society* 1-18, p. 3.

30 *Supra* n. 27, p. 2.

31 *Supra* n. 28, p. 85.

32 *Supra* n. 27, p. 3.

33 See "track your mood & get anonymous support" available at http://moodpanda.com (accessed 5 December 2017).

34 See "Everyone. Every run" available at https://runkeeper.com/index (accessed 5 December 2017).

35 See "Weight loss that fits" available at: https://www.loseit.com/ (accessed 5 December 2017).

collecting information about oneself.[36] However, there are various differences between the collection of this information in the past and the present. Recently, personal data are collected digitally, and stored online in large databases, which give room for many changes to the method of collection. First of all, the quantity of the collected data is possibly unlimited when data are available online, which is not the case for data that only exist in the real world (e.g. in a diary). This makes it much easier to collect large volumes of data from many individuals. Furthermore, data that are available online can be shared and multiplied easily, whereas real or physical data normally has only one owner. Thirdly, online databases can be combined into an unlimited database with very detailed knowledge about individuals. Finally, there may be apps on a smartphone or smart watch that collect all of the data that they are able to collect. All these new elements come together in an example concerning the app Strava.[37] Strava can be used to record running and cycling training sessions, to share these with your friends. Imagine you use this to trace your running speed. Strava shows you your running speed per segment, your pulse, your average speed, the amount of calories you have burnt, your route on a map, the time you have been active and everything else that is relevant about your run. Moreover, Strava shows how well you did in comparison to other users, your friends, people of the same gender, all runners on a specific segment in a specific time frame (a day, year, ever) and whether you have run a personal record or not.[38] This is a great deal of information. Strava even markets this on its website: "[Strava] compiles all performance data that you can imagine".[39] Once you have uploaded your

---

36 *Supra* n. 28, p. 85; *supra* n. 29, p. 2.

37 See "Strava" available at https://www.strava.com/ (accessed 5 December 2017).

38 See for an overview of all possibilities of Strava: "Features" available at https://www.strava.com/features (accessed 5 December 2017).

39 *Ibid.*

running activity on Strava, your contacts can react to it, give you kudo's for it, or share their own training sessions with you. Finally, Strava uses the data about your running habits to create a map of exercise routes, which are sold to individual members.[40]

## 3 Freedom, Autonomy, and Privacy

Every society needs rules that help to protect the individual's freedom.[41] The GDPR is the newest addition to the legal framework described in section one. Before we can assess whether or not the GDPR affects the influence of QS on an individual's freedom, it is important to see what we are talking about when we discuss privacy, freedom and autonomy. I discuss these three notions because they are interrelated. In fact, they may be seen as different aspects of the overarching concept of *human dignity.* This dignity is based on the idea that every human being has a right to be valued and respected. Moreover, it means that every individual is free to decide who he or she wants to be and "to pursue one's rights, claims, or interests in daily life so that one can fully realize talents, ambitions, or abilities as one would like."[42] Here, we can already see that freedom is part of human dignity since it is about the chances for an individual "to be *free* to develop his own personality to the fullest".[43] The freedom mentioned in the GDPR should thus be seen as a reference to human dignity, or a combination of freedom, autonomy and privacy. As is shown later in this article, QS can reduce an individual's freedom, autonomy and privacy.

---

40 See Mike Wehner, "Strava Begins Selling Our Data Points, and No, You Can't Opt-out" [2014] *engadget,* available at https://www.engadget.com/2014/05/23/strava-begins-selling-your-data-points-in-the-hopes-of-creating/ (accessed 5 December 2017).

41 Alan Westin, *Privacy and Freedom* (London: The Bodley Head, 1967) p. 23.

42 Edward Eberle, "Human Dignity, Privacy, and Personality in German and American Constitutional Law" (1997) 4 *Utah Law Review* 963-1056, p. 964.

43 *Ibid,* p. 965. This is also very clearly a Kantian idea.

*Privacy* is a difficult concept, without one clear meaning.[44] It expresses the idea that every individual should be able to decide who they allow to come into their private sphere. This private sphere exists of different levels: from your head, to your body, house, electronic devices, etc. Informational privacy is the idea that an individual has the right to decide who knows what about him or her. This is important because knowledge about a person implies a certain amount of power over that person. It is thus related to the idea that an individual can "claim […] to determine when, how, and to what extent information is communicated to others".[45] *Autonomy* means setting "your own laws".[46] *Freedom* is the ability to do as one wants to do. According to Kant, every individual has freedom to act.[47] Of course, there may be certain limits to an individual's freedom. Think for example of laws: some things are forbidden and thus people are not free to act, or they will, at least, be punished when they do act. Some philosophers, such as Steiner, also argue that people are limited in their freedom when their actions are forced by "physical means or by moral laws".[48] Steiner claims that a man cannot "call his actions his own, seeing that he is driven to them by a force other than himself".[49] The European ideas on freedom are based to a large extent on Kant's philosophy. According to Kant, freedom and autonomy are linked. Kant even understands freedom as autonomy. He does not understand freedom as being free from interference by others, but as following laws created and laid down by

---

44 Daniel Solove, *Understanding Privacy* (Cambridge: Harvard University Press, 2008) p. 1.

45 *Supra* n. 41, p. 7.

46 Auto (αὐτο) means self and nomos (νόμος) means law.

47 Paul Guyer (ed), *The Cambridge Companion to Kant and Modern Philosophy* (Cambridge: Cambridge University Press, 2006) p. 345.

48 Rudolf Steiner, *The Philosophy of Freedom,* (Rudolf Hoernlé tr, Susses: Rudolf Steiner Press, 1916) p. 40.

49 *Ibid*.

oneself.[50] However, this does not mean an individual can do anything that he or she wants to do. Just as laws can limit an individual's freedom, Kant says it is necessary that a person reflects on his or her desires, and, if necessary, acts opposite to them. He explains: "that choice which can be determined by pure reason is called free choice. [...] Human choice, however, is a choice that can indeed be affected but not determined by impulses, […] but can still be determined to actions by pure will."[51] Kant concludes that freedom is the availability to answer the question "what I ought to do". When the answer to this question is found, an individual acts freely and autonomously. Kant sees this as autonomy, because then individuals are truly able to see themselves.[52] To know how one ought to live, every individual should evaluate his or her motivations for action. This evaluation happens with the application of the *categorical imperative* to an action.[53] This categorical imperative consists of three elements: "act only according to that maxim whereby you can at the same time will that it should become a universal law";[54] "act in such a way that you treat humanity, whether in your own person or in the person of any other, never merely as a means to an end, but always at the same time as an end";[55] "act [in such a way] that your will can regard itself at the same time as making universal law through its maxims".[56] This last element of the categorical imperative implies that autonomy is necessary to act in freedom, according to Kant. To give an example:

---

50 Robert Johnson and Adam Cureton, "Kant's Moral Philosophy" [2016] *Stanford Encyclopedia of Philosophy*, available at https://plato.stanford.edu/entries/kant-moral/ (accessed 5 December 2017).

51 Immanuel Kant, *Groundwork of the Metaphysics of Morals* (Thomas Abbott tr, London: Longmans, Green and co, 1895) at 6:214.

52 Immanuel Kant, *Kritik der Praktischen Vernunft* (Riga: Hartknoch, 1788) ch 1.

53 *Supra* n. 51.

54 *Ibid.*, at 4:421.

55 *Ibid.*, at 4:429.

56 *Ibid.*, at 4:431.

Kant basically states that every individual should act according to the rules that he or she would wish all other people to follow as well, even though this might not be the most pleasant choice to make. Now imagine that I want to lie to someone, to benefit from it. My maxim (rule to follow) would then be: it is permissible to lie to people when you benefit from it. However, if this was a universal rule, it would not make sense, because if everyone can always lie, then what is the truth? Accordingly, this maxim cannot be a universal rule, and therefore I should not lie.

Kant therefore clearly links freedom with autonomy. As well as freedom and autonomy, freedom and privacy are also linked to each other. Westin described that "each individual is continually engaged in a personal adjustment process in which he balances the desire for privacy with the desire for disclosure and communication".[57] In line with this, Solove states that privacy is "an essential issue for freedom".[58] Thus, the decision to share or not share information with persons enhances an individual's freedom.

Now we know what the scope and meaning of the central notions in this article are. All of these elements refer back to the overlapping notion of human dignity. The next parts discuss how QS can negatively influence freedom and therefore interfere with your life. The term 'freedom' is used, but this refers to both freedom and autonomy, and is closely linked to privacy. Later in the article, a distinction is made between external and internal freedom. This will be explained further in section 5. However, first it is time to have a more detailed look at the GDPR.

---

[57] *Supra* n. 41, p. 7.
[58] *Supra* n. 44, p. 2.

## 4 The GDPR and QS

The GDPR regulates the "protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data".[59] Personal data refers to any information "relating to an identified or identifiable natural person". A person is identifiable when he or she can be identified directly or indirectly.[60] This implies that the GDPR is applicable to most QS tools, since these apps combine different data such as physical factors, location, and economic or social identity, which are all mentioned as identifiers in the GDPR.[61] Moreover, to use the apps that collect data that create a person's QS, users usually have to be logged in to the app platform (although, of course, there can be exceptions to this). This log-in can also be an identifier.[62]

The GDPR applies to the processing of personal data,[63] but there are some exceptions to its applicability. One of these is the processing of personal data "by a natural person in the course of a purely personal or household activity".[64] This does not mean that the GDPR is not applicable to QS, since the processing normally does not take place by a natural person, but by the company providing the QS-tool. Therefore, the GDPR is applicable in the situation of QS.

Relevant for QS is article 3 of the GDPR, which states that it is not important whether or not the actual processing takes place in the Union, when its context is "the context of the activities of an establishment of a controller or a

59 GDPR, art. 1(1).
60 *Ibid*., art. 4(1).
61 *Ibid*.
62 *Ibid*., rec. 26.
63 *Ibid*., art. 2(1).
64 *Ibid*., art. 2(2)(c).

processor in the Union".[65] This means that the GDPR is also applicable to QS-tools that are created in third countries and used by European citizens.

Another important element of the GDPR is that the processing of personal data is only allowed if a number of conditions are met.[66] Article 6 gives, among others, the following conditions: the data subject gives his or her consent to the processing; it is necessary for "the performance of a contract to which the data subject is party" or it is necessary for "purposes of the legitimite interests pursued by the controller".[67] Compared with the EDPD, there is a small difference, since the current EDPD asks for *unambiguous consent*,[68] whereas the GDPR asks for *consent*.[69] Although this might seem to imply that the GDPR will be less strict regarding consent, this is absolutely not true. Actually, the definition of consent is tightened and its role is strengthened in the GDPR.[70] In the article regarding definitions, consent is described as: "'any freely given, specific, informed and *unambiguous* indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her."[71] In recital 32 it is explained even further: the consent should be given by a clear affirmative act, it should be freely given, specific, informed and unambiguous. In addition, there are limitations set: silence, pre-ticked boxes or inactivity do not constitute consent.[72]

---

65 Ibid., art. 3(1).
66 *Supra* n. 21, p. 318.
67 GDPR, art. 6.
68 EDPD, art. 7.
69 GDPR, art. 6.
70 Claudia Quelle, "Not Just User Control in the General Data Protection Regulation. On Controller Responsibility and How to Evaluate Its Suitability to Achieve Fundamental Rights Protection", in Anja Lehmann, Dianne Whitehouse, Simone Fischer Hübner, Lothar Fritsch and Charles Raab (eds) *Privacy and Identity Management. Facing up to Next Steps* (IFIP Summer School 2016, Berlin: Heidelberg, 2017) p. 4.
71 GDPR, art. 4(11).
72 See: GDPR, Recital 32.

Thus, according to the GDPR, consent must be unambiguous and given either "through a statement or a clearly affirmative action".[73] This is stricter than the rules regarding consent in the EDPD. The EDPD requires that consent must be given unambiguously and freely, but the GDPR adds to this 'freely given' that "[w]hen assessing whether consent is freely given, utmost account shall be taken of whether, inter alia, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract."[74] Recital 43 adds that there cannot be freely given consent if the situation is a "take it or leave it"-one.[75] Furthermore, since unambiguously is no longer part of the article related to consent, but of the definition of consent, every rule that falls under the GDPR also requires unambiguous consent.[76] Finally, the GDPR adds more categories for which explicit consent is required.[77] However, health was already included in the EDPD.

Two elements of the GDPR may cause problems for QS-tools. Firstly, there are two problems related to the 'consent' that is asked for in the GDPR. The first is related to the prohibition concerning the processing of "data concerning health".[78] Data concerning health are any "personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status".[79] Recital 35 gives a very broad explanations of data concerning health, that includes "data

---

73 *Supra* n. 70, p. 4.
74 GDPR, art. 7(4).
75 GDPR, Recital 43; *supra* n. 70, p. 4.
76 For example the ePrivacy Directive does not require unambiguous consent at the moment, because the EDPD does not define consent as unambiguously in its definition of consent.
77 See: GDPR, art. 8.
78 See: *Ibid.*, art. 9, with exceptions in 9(2)(a) and 9(2)(e).
79 *Ibid.*, art. 4(15).

pertaining to the health status of a data subject which reveal information relating to the […] physical or mental heatlh status of the data subject".

Because of the specific nature of (most) QS-tools, that do collect these types of data related to health, this can be problematic. As in the example of Strava, where data about the pulse and physiological state of individuals are shared. Although there is a basic prohibition of the processing of data related to health, there are some exceptions. These are similar in the GDPR and the EDPD.[80] One of these is when the individual concerned gives his or her "explicit consent" for the processing of these data.[81] In fact, it is likely that this exception is applicable to any QS-application.[82] QS-users do consciously choose to download and use certain apps. Although there can be trouble with the acceptance of general conditions (the issue of consent is discussed further in section 5), QS servers should just ask for this explicit consent and then they act in accordance with the GDPR. Another problem related to consent seems more difficult to overcome. Most QS-tools collect data that are not only related to the individual user, but also to other users. This element will be discussed in greater detail in section 5 as well, but for now it is enough to know that data are used to compare the achievements of different users with each other.[83] Therefore, it might be the case that specific data of an individual is shared with other persons. It is questionable whether users have given consent for this specific use of their personal data.[84]

Secondly, another problem with QS and the GDPR is related to the fact that data collected in a QS-application, cannot be used for other purposes. The GDPR requires that personal data is collected for specific, explicit, and legitimate

---

80 *Supra* n. 21, p. 318.
81 GDPR, art. 9(2)(a).
82 *Supra* n. 21, p. 318.
83 *Ibid.,* p. 317.
84 *Ibid.*

purposes. Moreover, the data collected should not be processed in a way that is incompatible with these purposes.[85] However, when an individual consents to the processing of his or her data to learn how to lose weight, or run a marathon, it is not immediately clear that that individual has also given consent to use his or her data for other reasons, such as advertising or comparison with other users. Like before, where it is unclear whether consent is given to share and compare the data that are collected, it is unclear whether the consent that is given when users download a QS app or register on a platform is enough to include every use of their data.

## 5 QS, Freedom, and the GDPR

This section will show first of all how the QS influences freedom. QS does not usually stop after having collected personal data. These data will be processed in order to be able to say something about them. Therefore, personal data will be processed and conclusions will be drawn from these statistics. The different steps that are normally used to process data collected with QS are described. These steps are: comparison, creation of group norms, standard-setting (internal restriction of freedom), and judgments on the basis of data (external restriction of freedom). Secondly, in every step, it is shown how the GDPR can or cannot help to protect an individual's freedom in that specific regard. The GDPR aims to protect the personal data and privacy of individuals, but is this enough to protect their freedom? Of course, not all data that are collected with QS are processed in exactly the same way. However, the statements made in this section are applicable to most data.

---

[85] See: GDPR, art. 5(1)(b).

### 5.1 Comparison in Three Ways

There are different possibilities on how to compare the processed data. First, a person's data can be compared to the data of other users. This can be online on a forum, through a community, or in the app itself, when the data collected is compared to data of other users.[86] This means that you will see how well you have been doing, in comparison to the other users of the same application. Secondly, personal data can be compared to a user's own previous data. Here, you will see whether you did better than last week: whether you ran faster, smoked less or slept better this week than last week. Thirdly, the data can also be compared against someone's desired goal.[87] A QS device then acts as a surveilling machine to evaluate and discipline an individual to change his or her behaviour.[88] So the app will compare you to the statistics that are needed to reach your goal and tell you whether or not you have to change your behaviour. In these different comparisons, the QS-tool will collect data about an individual, process these and then compare with other users, the individual himself or the desired goal. The QS-tool will gain knowledge about a person's behaviour through an analysis of his or her data. Feedback is given to help reaching a certain goal. Research shows that especially in sport situations, goal-setting is very effective. This is because goal–setting in general works very well for persons, but especially in sport situtations, because measurement of performance is easier than in other organisational settings.[89]

---

86 Often, this will be an individualised comparison: for example, only the running speed of other female users between 20 and 25 will be compared with your data.

87 *Supra* n. 26, p 10.

88 Katleen Gabriels, "I Keep a Close Watch on this Child of Mine" (2016) 18(3) *Ethics and Information Technology* 175-184, p. 175.

89 Edwin Locke and Gary Latham, "The Application of Goal Setting to Sports" (1985) 7 *Journal of Sport Psychology* 205-222, p. 206.

Since most QS-users do so to improve some aspects of their life (eat healthier, become fitter, run faster),[90] this comparison will add more elements to an already existing feeling of failure or success. Different questions arise with the knowledge that personal data are being compared in these three different ways. First of all, how detailed are those categories in which persons are sorted? Think about: does it only compare on the basis of gender and age or more? And is the age-division between 25 and 40 or between 25 and 27? Secondly, how transparent are these categories, and is it possible to find out how many other people there are in a specific category? And last but not least: can an individual decide which data are used to compare, or does a QS-device compare all data automatically? Although it can be far from transparent how an app builds up these categories, they are very important. The group that is used as a norm or reference can be very different based on the criteria for inclusion. This determines the yardstick or the standards according to which a person is assessed.

### *5.1.1 Comparison and the GDPR*

The GDPR has a few rules on these categories. The GDPR obliges processors to be pseudonymised in order to be processed lawfully.[91] This implies that at least other parties, and perhaps also the processor, cannot relate data back to a specific user, once the data are used for comparison. However, several authors wonder whether pseudonymisation actually leads to anonymity.[92]

---

90 *Supra* n. 26.

91 GDPR, art. 6.

92 See for example Harald Gjermundrød, Ioanna Dionysiou, and Kyriakos Costa, "PrivacyTracker: A Privacy-by-Design GDPR-Compliant Framework with Verifiable Data Traceability Controls" in Sven Casteleyn, Peter Dolog and Cesare Pautasso (eds) *Current Trends in Web Engineering,* (ICWE 2016 Workshops, Berlin: Springer International Publishing, 2016) pp. 3-15.

Regarding the creation of the categories, it is clear that QS-data of a specific individual will be used for comparison with the data of other users. This does not only entail that every individual receives information about other users, but also that all data are compared to the data of other users. It is questionable whether the specific consent of users is asked to do so, and therefore it is not clear whether it is in line with the GDPR to process data of users for this purpose. For example, in the privacy statement of MoodPanda, it is made clear that information is used to "measure and improve" their services over time.[93] However, no specific consent is asked for that. The privacy policy of RunKeeper even makes clear that it provides and shares information through its services.[94] By providing them with personal data, an individual is "consenting to [their] use of it in accordance with this Privacy Policy."[95] However, even here, it is not mentioned that these data are used for comparison with other users.[96] It might thus be questionable whether this is in line with the GDPR, since it requires that users give consent for any use of their data. It might therefore not be in line with the GDPR and EDPD, but the applications of MoodPanda and RunKeeper do use the data for this goal, although they do not refer to it explicitly. Under the current EDPD, this has not been enforced. However, the idea is that the GDPR will sanction more of these actions. Only time can show whether this will change under the GDPR. It can at least be concluded that the GDPR and QS appear to be inherently incompatible with regard to this point.

---

93 See "MoodPanda Privacy Policy" available at http://moodpanda.com/privacy.aspx (accessed 5 December 2017).

94 See "RunKeeper Privacy Policy" available at https://runkeeper.com/privacypolicy (accessed 5 December 2017).

95 *Ibid.*

96 *Ibid.* The only thing that is mentioned about other users is "to enable social-sharing, to find your friends, […] to allow you to communicate and interact with other users".

### 5.2 Group Norms

The yardstick that is used to compare data to a group is an interesting point to discuss further. Social norms are present in every society or group.[97] Research has shown that group norms often have a "powerful, and consistent, influence on group members' behavior."[98] This might be helpful, but the groups of users of most QS-applications are far from neutral, and it may be impossible to know who are included in the group. The latter element is described above: since you do not know anything about the categories, you do not know who belong to your 'group'. QS-users are not neutral or selected randomly. Self-trackers can be divided into several categories: sports enthusiasts, people who want to achieve a specific goal (such as lose weight, run a marathon, or quit smoking), people with certain medical conditions, and people who are interested in documenting their life.[99]

Most of these users aim at improvement of a certain condition. Therefore, these people will produce data that differ from the average data if you were to look at an entire society, or at least a randomised group of people: people who want to lose weight, typically eat less than other people and people who want to run a marathon will train harder than average. So, people do not only share their data, but also (implicitly or explicitly) their values and goals.[100] This sharing has implications for people's perception of their body and 'productivity'. When

---

97 *Supra* n. 41, p. 13.

98 Daniel Feldman, "The Development and Enforcement of Group Norms", (1984) 9(1) *The Academy of Management Review* 47-53, p. 47; Richard Hackman, "Group influences on individuals" in Marvin Dunnette (ed) *Handbook of Industrial and Organizational Psychology*, (Chicago: Rand McNally, 1976) pp. 1455-1525.

99 S*upra* n. 26, p. 6.

100 *Supra* n. 25, p. 27-28.

someone tracks his or her productivity and health, an illness or a goal that has not been reached can be seen as a failure of efficiency or self-control.[101]

In a group of QS users, different things can happen when data are shared. Here we first have to make a distinction between QS-tools that make it possible to decide whether or not to share a certain achievement and apps that do not give that option.[102] When people can decide to share or not, this can change the group norms. A beginner or new member of the app can then feel like he or she will never be able to be succesful, since the group has set a very high standard by only sharing their best scores. This can make people either very motivated and stimulated to reach the same goals,[103] or let them be turned off because of the unrealistic goals. This is also shown in research that found that long-term goals are difficult to reach without short-term goals. If an individual only has this long-term goal (or the very high standard), he or she may end up in "viewing the end-goal as beyond one's capability to attain or to take seriously".[104] This is also related to the fact that when individuals do not see enough progress in relation to their goal (or the standard they want to achieve), the goal-setting stops working.[105]

Secondly, it can be that people have to share all their data. This will lead to a more balanced reality, since it does not only show people's topscores, but also their off-days. This might make it easier to begin using an app, since everyone has been a starter, and those data are available as well.[106] However, it can also make the group norm even more pressing, because all other users can

---

101 *Ibid.*

102 For example in Strava, you can view your performance after running or cycling and then choose whether or not you want to share this with your friends and followers.

103 See for example *supra* n. 21, p. 316.

104 S*upra* n. 89, p. 207.

105 *Ibid.*

106 *Ibid.*

see when you did not do well for a week. Since one of the main functions of a group norm is to legitimate the power of the group over individual members, these norms can become very pressing, especially if an individual does not meet the standard.[107] This can also make people feel either less motivated because they always have to be the best version of themselves, or make them turn off because it is impossible to always achieve a new topscore.

So, there are roughly two main options: people will either become more motivated, or more likely feel disappointed because they cannot live up to the group standard. These group norms will therefore at least be an influential factor in one's decisions. From now on, this article will focus on persons that try to follow the group norms.

#### *5.2.1 Group norms and the GDPR*

It is difficult to link the creation of group norms as described above to the GDPR. In my opinion, this is ultimately related to profiling or self-profiling. Profiling is "the process of discovering correlations between data in databases that can be used to […] identify a subject as a member of a group or category".[108] This means that self-profiling, in the sense of creating the norms that are used to identify a group, can be seen as a way of profiling. However, it is questionable whether the GDPR also protects the self-profiling that leads to the creation of group norms. This is questionable because it is an action of individuals themselves. But on the other hand, the GDPR does broaden the rights of the subject with regard to profiling. Article 20 for example gives a right not to be subject to a measure based

---

[107] *Supra* n. 98, p. 49. For more information, see Daniel Katz and Robert Kahn, *The Social Psychology of Organizations* (New York: Wiley, 1978).

[108] Bart Schermer, "The Limits of Privacy in Automated Profiling and Data Mining" (2011) 27(1) *Computer Law & Security Review,* 45-52, p. 45.

on profiling.[109] A fair conclusion might therefore be that the GDPR has only a little to say about the creation of group norms.

## 5.3 Internal Restriction of Freedom

### *5.3.1 Following the Standard*

As discussed above, group norms can be created by a QS app. But how can these norms influence people's behaviour? Apart from the hereinafter mentioned research, not much practical evidence exists on the restrictions to internal freedom. However, this does not mean that it cannot be an issue. There are strong arguments, which are put forward in this section, to suggest that internal freedom can be restricted because of QS. Research has shown that people look to others to guide their actions.[110] When looking at QS, a user can be interested in two questions about those others. Firstly: what do other users say that one *should do*, and secondly: what do other users actually *do* in the same situation?[111] Both questions can easily be answered in QS: for example, a forum or notification will tell what to do, and data of other users shows what they do. It is therefore easy to rely on others to determine what is 'right'. This reliance is even stronger when the reference group is seen "to be motivated and competent".[112] Consequently, a QS app can be very convincing in giving a user a new standard that should be followed. So a new standard can easily be created by a QS-tool, but why would

---

[109] *Supra* n. 15, p. 69.

[110] Solomon Asch, "Effects of Group Pressures Upon the Modification and Distortion of Judgments" in Greg Swanson, Theodore Newcomb, and Edward Hartley (eds.) *Readings in Social Psychology*, (New York: Holt, Reinhart & Winston, 1952) pp. 393-401; John Turner, *Social Influence*, (Milton Keynes: University Open Press, 1991).

[111] Matthew Hornsey Louise Majkut, Deborah Terry and Blake McKimmie, "On Being Loud and Proud: Non-Conformity and Counter-Conformity to Group Norms" (2003) 42(3) *The British Psychological Society* 319-335.

[112] *Ibid*, p. 320.

people follow this new standard?

There are different reasons why these standards influence people so heavily. Firstly, people can feel unconfident about what to do, and therefore use others to determine what the right thing is to do. Secondly, these norms can tell people how they can fit in with the majority in order to become accepted.[113] This is very much linked to autonomy, as dicussed in section three. In theory, people are free to design their own life, but this is a huge responsibility. Therefore, people are looking for the group to design standards for their life. However, everybody is free to choose his or her own norm.

Due to uncertainty, people are likely to follow a new standard that has been set both by the users of the QS tool, or by the QS-tool itself. This is because, as explained earlier, the QS-tool uses data-analysis to compare one's data on three different levels: previous scores, other users, and a person's goal. So the norm is not only set by what other users do or should do, but also by what *you* do or should do, based on the feedback you receive from the QS-analysis.

This new standard that an individual feels he or she should follow, changes his or her reference framework. This can occur without the person really being aware of it. Because only specific persons use an app, the standard given in such an app, is not 'the average'. This can lead to a tunnelvision, in which a user may think that his or her scores are not good enough, although they are in fact much higher than those of most of the other people. This standard that an

---

[113] See for a good example the research done by Deutsch and Gerard in 1955, where participants were required to judge the length of two lines. Some respondents were instructed to give the wrong answer. The study suggested that the pressure to comply with the majority was very high for participants who were not aware of the fact that some respondents were instructed to do so (see: Morton Deutsch and Harold Gerard, "A Study of Normative and Informational Social Influences Upon Individual Judgment" (1955) 51(3) *Journal of Abnormal and Social Psychology* 629-636). Various other researches have shown that people are not willing to speak out to the majority in general.

individual imposes on him- or herself, can thus be unrealistic and far too high. By following this standard, an individual can limit his or her own freedom and autonomy rigorously. Lupton has for example described the challenges related to eating healthy.[114] This research shows that health has become a right and a duty, in which individuals must choose well what to eat.[115] This happens because the media and professions create certain norms about which food is healthy. However, these norms on healthy food may result in obsession with healthy food, which takes away people's freedom to decide on what to eat and how to act (together with eating healthy comes a very active life).[116]

Although this obviously can restrict a person's freedom, it is still a choice to become subject to the discipline of QS. In this way, it is possible to say that the QS app maybe limits your *internal* freedom to behave as you want to - but you are still free to choose not to do so. In addition, all of the internal freedom limitations are technological features which can be opted out of and which have always existed in other forms. An example of this is the social pressure an individual can feel to conform to beauty standards. This pressure already existed before the technologies that form QS were created. QS is comparable with beauty standards. It is an even more powerful and strong standard that can restrict an individual's internal freedom. This is not only because QS provides for an opportunity to collect more (all) data about a certain issue or a certain individual, which makes it much more personal and potentially more infringing on the status of a certain individual. There is a great difference between a beauty

---

[114] Deborah Lupton, "Food, Risk and Subjectivity" in Simon Johnson Williams, Jonathan Gabe and Michael Calnan (eds) *Health, Medicine, and Society. Key Theories, Future Agendas* (London: Routledge, 2000) pp. 205-217.

[115] Cristian Rangel, Steven Dukeshire and Letitia MacDonald, "Diet and Anxiety. An Exploration into the Orthorexic Society" (2012) 58(1) *Appetite* 124-132, p. 124.

[116] Guido Nicolosi, "Biotechnologies, Alimentary Fears and the Orthorexic Society" (2006) 2(3) *Tailoring Biotechnologies* 37–56.

standard that exists and is equal for everyone, and a personalised standard that counts everything an individual does. QS cannot be 'fooled' because of technological progress. This is related to the difference between a human coach and a phone with QS, which is mentioned in section 5.3.2, and also in section 2. Moreover, QS is less visible, more hidden, and even more merciless than other social structures that can limit an individual's internal freedom.

### *5.3.2 Internal Freedom and the GDPR*

This form of restriction is already known in literature (see e.g. literature about behavioural targeting[117] and filter bubbles[118]), but has never been linked to QS. So far, it has predominantly been linked to online surfing behaviour. These problems, however, are not solely related to the tracking of online surf behaviour and Internet searches. The same phenomenon can occur when using QS apps, as is described above. This is a relatively unknown and unseen problem, because the GDPR focuses mainly on processing of data, and on use by third parties. This is very important, but the problem with internal restriction of freedoms seems to occur earlier: in the phase where the data are collected. It can easily remain unclear what comparison is made, what reference group is created or what algorithms underlie the comparison. The GDPR does contain a right for the data subject to obtain access to information about the existence of automated decision-making, including profiling. This includes "meaningful information about the

---

[117] Frederik Zuiderveen Borgesius, *Improving Privacy Protection in the Area of Behavioural Targeting* (2015) available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2654213 (accessed 5 December 2017); Avi Goldfard and Catherine Tucker, "Online Advertising, Behavioral Targeting, and Privacy" (2011) 54(5) *Communications of the ACM* 25-27.

[118] Frederik Zuiderveen Borgesius et al., "Should We Worry About Filter Bubbles?" (2016) 5(1) *Internet Policy Review: Journal on Internet Regulation* 1-16; Eli Pariser, *The Filter Bubble: What the Internet is Hiding from You* (London: Penguin Press, 2011).

logic involved".[119] This could help individuals to receive some information about their data-comparison. However, there are some reasons why this right may not be as successful as suggested. First of all, there are authors who doubt whether or not this right on information is legally existing and feasible.[120] Feasibility is doubted because the right lacks precise language and does not contain any safeguards. The existence is doubted because article 22(3) of the GDPR only mentions a right to "implement suitable measures to safeguard" and not a right to explanation. Secondly, if this right to information would be feasible and existing, it would be about automated decision-making. With internal freedom restriction, in the end an individual restricts his or her freedom, based on information from the QS-tool that is created with an algorithm. Therefore, the right to information would not be applicable to the situation of internal freedom-restriction. Finally, it is questionable how much information would be shown to a data subject. This is because the privacy of other individuals should not be infringed by the request for information.

It can be questioned whether the purpose of achieving one's own goal includes comparison with other user's achievements (and re-use of your data to determine the standards for others). Accordingly, it is questionable whether or not the consent given to the QS app can fulfil the demands of the GDPR. How could you ever consent to have your internal freedom restricted, if you cannot know the underlying logic that the app uses to create the standards that you set for yourself? This is all the more worrying if the risks for physical and emotional

---

[119] GDPR, art. 15(1)(h).

[120] Sandra Wachter, Brent Mittelstadt and Luciano Floridi, "Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation" [2017] *International Data Privacy Law* 76-99.

well-being are taken into account; not being able to meet your own standard is not particularly helpful for you self-confidence.[121]

This is something that is important to be aware of. It might be necessary to create a debate about the question of whether the GDPR should protect this type of internal freedom in order to protect individuals from harming their physical and/or mental health by trying to achieve unrealistic goals. This is very different with an online QS tool than for a human coach. A coach can bring a human factor to the evaluation by showing empathy and understanding.[122] QS only consists of hard data that are supposed to speak for themselves. Incorrect interpretations of these data by an uneducated individual can lead to incorrect or dangerous decisions, whereas a coach can always look at the human behind the data and help to interpret. I can understand how it can be seen as paternalistic or over-protective to protect people against restrictions of their internal freedom. However, it is at least important that people are aware of this influence of QS. Perhaps the debate about information bubbles can be expanded to include QS and freedom.

## 5.4 External Restriction of Freedom

### *5.4.1 Judged on Your Data*

One step further than restricting an individual's freedom to choose, is the

---

[121] The concepts of consent and purpose limitations have been discussed in a plethora of works. These include: Menno Mostert, Annelien Bredenoord, Monique Biesaart and Johannes van Delden, "Big Data in Medical Research and EU Data Protection Law: Challenges to the Consent or Anonymise Approach" (2016) 24 *European Journal of Human Genetics* 956-960; Beata Safari, "Intangible Privacy Rights: How Europe's GDPR Will Set a New Global Standard for Personal Data Protection" (2017) 47(3) *Seton Hall Law Review* 809-848; Tal Zarsky, "Incompatible: The GDPR in the Age of Big Data" (2017) 47(2) *Seton Hall Law Review* 995-2012.

[122] Sander Voerman, "Health Coaches" in Linda Kool et al (eds) *Sincere Support. The Rise of the E-coach,* (The Hague: Rathenau Instituut, 2015) p. 41.

situation in which other people judge him or her on the basis of a QS-profile. This means that others restrict a person's freedom (*external* restriction of freedom), because they limit his or her options based on the data they have. One can think about very different situations here. One is a situation in which friends or members of a group judge an individual on the basis of his or her achievements in a QS-tool. This can be very harmful for a person, especially when it influences a person's social status.

In addition, it may be possible that companies or other private parties judge persons on the basis of their data. One example is insurance companies that offer a discount for healthy living when you share your data. Another example is a typical American phenomenon called workplace wellness programmes. These programmes seek to "help employees improve their health and fitness levels, often by offering incentives to employees who participate in various program activities or achieve certain health-related goals".[123] Employees must provide health information for these programmes, which can relate to walking groups, losing weight, lowering blood pressure, managing illnesses such as asthma or quitting smoking. These programmes reward either employees that show improvement or employees that achieve a certain goal. However, the latter system is debatable, since it might be discrimination on health. Some of these programmes are also linked with insurance companies, where employers can receive health insurance benefits.[124] When these programmes are linked with insurance companies, this can be very harmful for a person's freedom. This might

---

[123] Lisa Guerin, "Is Your Employee Wellness Program Legal?" available at http://labor-employment-law.lawyers.com/human-resources-law/wellness-programs-may-be-bad-for-employers-health.html (accessed 5 December 2017); Soeren Mattke et al., *Workplace Wellness Programs Study* (Final Report, Santa Monica, CA: RAND Corporation, 2013).

[124] Michelle Mello and Meredith Rosenthal, "Wellness Programs and Lifestyle Discrimination – The Legal Limits" (2008) 359 *The New England Journal of Medicine* 192-199.

be especially true when the personal data are shared with insurance companies in order to receive a discount.[125] Although research has shown that workers are enthusiastic about assistance and guidance to improve their health,[126] some cases on misuse of personal data by corporations have made Europe careful in approving these types of programmes.[127] However, worksite health and wellness programmes are also an existing phenomemon in Europe.[128] In particular, the European Agency for Safety and Health at Work (EU-OSHA) focuses on this. They target topics such as eating healthy at work, mental health, exercise at work and longitudinal health monitoring.[129] At present, they are not linked to insurance companies.

The fact that this does not happen, does not mean that other companies cannot judge individuals on their data in Europe. Some of the data collected via QS can be extremely interesting for marketeers and companies.[130] And what will happen when a company combines data from different apps? Is this a nice way of receiving the most accurate offers, or is this a privacy-infringement? Regardless of which one of the two it is, it still influences that person's freedom. It is not only marketeers that might be interested, governments, social organisations and cybercriminals can, all for different reasons, benefit from QS-data.[131] When these organisations receive data that an individual has collected using a QS-tool, they do not only know what he or she did, eat or sleep like, they

---

125 *Ibid.*

126 Wolf Kirsten, "Making the Link between Health and Productivity at the Workplace —A Global Perspective" (2010) 48 *Industrial Health* 251-255, p. 254.

127 See for example "Daimler Speicherte Heimlich Krankendaten" (2009) *Der Tagesspiegel* available at http://www.tagesspiegel.de/wirtschaft/neuer-datenskandal-daimler-speicherte-heimlich-krankendaten/1497042.html (accessed 5 December 2017).

128 Marco Guazzi et al., "Worksite Health and Wellness in the European Union" (2014) 56(5) *Progress in Cardiovascular Diseases* 508-514

129 *Ibid,* p. 510.

130 *Supra* n. 26.

131 *Ibid.*

also might know what his or her goals are, how well he or she is doing, what his or her weakness is and so on. This gives them a very powerful set of knowledge about individuals, and knowledge is power. When they use this against the individual, it can truly limit his or her freedom to choose. This is accurately described by Schwartz: "Decisional and information privacy are not unrelated; the use, transfer, or processing of personal data by public and private sector organizations will *affect the choices that we make*."[132]

Finally, not only companies but also governments might be very interested in data. This does not mean that governments can use the QS, but they may access QS technologies for their own purposes or access data collected with QS. Although this is probably unimaginable in Europe, in China, the Communist Party is working on a so-called 'social-credit system'.[133] The aim of this plan is to influence the behaviour of the Chinese. Behaviour is tracked and then a punishment or reward can follow. Awards are, for example, money, a higher pension, better health insurance or priority for public housing.[134] Data that are collected come, for example, from monitoring through cameras, online data collecting and databases.

All of these examples show that there are many parties that have an interest in personal data, especially the more sensitive or private data that is targeted specifically by QS-tools. These data that are collected by individual users are analysed. This allows interested parties to find specific patterns or correlations between different datasets, or to deduce new information from the

---

132 Paul Schwartz, "Property, Privacy, and Personal Data" (2004) 117(7) *Harvard Law Review* 2055-2128, p. 2058.

133 The Economist, "China invents the digital totalitarian state" (2016) *The Economist* available at https://www.economist.com/news/briefing/21711902-worrying-implications-its-social-credit-project-china-invents-digital-totalitarian (accessed 5 December 2017).

134 *Ibid.*

data.[135] On the basis of the data collected, parties can try to predict and judge behaviour. This can limit one's freedom in several ways. First of all, people can judge someone on the basis of what he or she does or does not do. Although this happens all the time in our society, and normally is not seen as problematic, this might be different when the information about an individual's actions is as detailed as it can be with QS. Secondly, persons may be excluded from certain offers, because they do not fit into a profile. And if a company or government knows a person's weak spots, based on data about food and mood, is it still ethical to target him or her in his or her weakest moments? This implies that you cannot even choose anymore, since someone else already did for you.

Moreover, it can be the case that persons get certain (dis)advantages on the basis of their data. Think about a discount for health insurance when living healthy, or a higher price when a change in diet proves unsuccessful. Imagine your health insurance provider sending you the following messages: "You have exceeded your fats quota this week; you don't adhere to your dietary goals: your insurance premium will rise".[136] It can definitely harm an individual's freedom when a health insurance premium can be increased if companies infer health problems from the user's fitness data and share this information with insurance providers, or when they can access the fitness data.[137] What insurers see as a great advantage of QS is that they can receive more data, in real time.[138] This decreases

---

135 Primavera De Filippi, "Big Data, Big Responsibilities" (2014) 3(1) *Internet Policy Review* 1-12.

136 Morgane Remy, "Personal Data: What if Tomorrow Your Insurance Company Controlled Your Lifestyle?" [2016] *Multinationals Observatory.*

137 Sourya De and Daniel Le Métayer, "PRIAM: A Privacy Risk Analysis Methodology (Research Report)" [2016] RR-8876, Inria – Research Centre Grenoble, Rhône-Alpes (hal-01302541). For an example, see Tara Siegel Bernard, "Given Out Private Data for Discount in Insurance" [2015] *The New York Times* available at https://www.nytimes.com/2015/04/08/your-money/giving-out-private-data-for-discount-in-insurance.html (accessed 5 December 2017)

138 *Supra* n. 136.

their uncertainty and increases the control over individual insurance policies. This is happening in Europe as well, although not yet for health insurance policies. But the European legal context can be seen as quite strict in the sense that it does offer protection for the data that insurance companies would want to collect. The GDPR has strict rules on personal data related to health, as explained above. However, this does not make it impossible for insurance companies to offer these kinds of benefits.

Even targeted advertising can affect the choices that we make. Therefore, when a company sends targeted advertisements, our free choice is affected by the fact that a company has assessed us on the basis of our data.

These risks described above are not hypothetical at all. Different authors have warned about the privacy challenges of self-trackers.[139] This implies there exist risks to users' privacy.[140] Many different people and businesses will be interested in the data. Creators of an app might therefore earn vast sums of money by selling personal data to interested parties.[141] People should be aware of the idea that many parties do have an interest in their data. And especially when an app is available for free, companies will earn money by selling personal

---

[139] See for example: Rajindra Adhikari, Karen Scott, and Deborah Richards, "Security and Privacy Issues Related to the Use of Mobile Health Apps", (2014) paper presented at the 25th Australasian Conference on Information Systems mHealth App Privacy and Security Issues 8th-10th Dec 2014, Auckland, New Zealand, available at http://www.colleaga.org/sites/default/files/attachments/acis20140_submission_12.pdf*25th* (accessed 5 December 2017); Hamed Haddadi, Akram Alomainy and Ian Brown, "Quantified Self and the Privacy Challenge in Wearables" [2014] *The IT Law Community;* Deborah Lupton, "Quantified Sex: a Critical Analysis of Sexual and Reproductive Self-Tracking Using Apps" (2015) 17(4) *Culture, Health & Sexuality* 440-453.

[140] Bari Faudree and Mark Ford, "Security and Privacy in Mobile Health" [2013] *CIO Journal* available at http://deloitte.wsj.com/cio/2013/08/06/security-and-privacy-in-mobile-health/.

[141] *Supra* n. 132, p. 2055: "Personal information is an important currency in the new millennium".

data.[142] This touches upon the earlier discussion on dignity; QS might result in reducing a person into a collection of data for only commercial purposes.

### *5.4.2 External Restriction of Freedom and the GDPR*

Many of the problems related to the limitations of external freedom are already mentioned in the literature. All of the problems mentioned here are related to QS. However, these have not all been linked to QS already before.

The first problem is that data in QS-tools are protected very poorly. This makes it highly possible that others can look at your data. A reason for this is that QS-apps work with low-cost data collection and communication systems. Security measures should therefore also be minimal and cheap.[143] This makes users sensitive to abuse, because third parties with no rights to the data can easily access the data or process the data for their own purposes. Although this is not a problem uniquely for QS, it does make users vulnerable to infringements of their external freedom, especially within QS because there are so many sensitive and personal data collected. Under the EDPD there is an obligation for Member States to provide appropriate safeguards.[144] However, McCarthy showed in 2013 that consumer data in eHealth apps (any mobile health application) is usually protected very poorly. In his study of 43 health and fitness apps, only 74% of the free apps had a privacy policy, only 25% of the free apps informed consumers about this privacy policy, and *none* of the free apps encrypted the data that

---

142 "If you are not paying for it, you're not the customer; you're the product being sold" – by Andrew Lewis available at https://twitter.com/andlewis/status/24380177712 (accessed 5 December 2017).

143 Tracey Caldwell, "The Quantified Self: a Threat to Enterprise Security?" (2014) 11 *Computer Fraud & Security* 16-20, p. 17.

144 EDPD, art. 6(1)(b).

consumers filled in.[145] It is questionable whether the GDPR will change this problem. The current EDPD obliges controllers to implement "appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access […] and against all other unlawful forms of processing".[146] This does not only apply to the controller or the processor but also to "any person acting under [their] authority".[147] Furthermore, controllers must ensure "a level of security appropriate to the risks represented by the processing and the nature of the data to be protected", with regard to "the state of the art and the cost of their implementation".[148] This can be seen as a risk-based approach to data security.[149] The GDPR contains some changes that are related to security. For example, article 25 of the GDPR adds new elements to the existing article 17(1) of the EDPD. These are "the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing".[150] General security requirements have remained largely unchanged. Together with article 32 of the GDPR, the requirement is that companies should achieve a level of security of data protection and privacy to EU citizens that is "appropriate to the risk".[151] However, the question is whether these rules actually result in secure data. This is partly because it is not clear yet what appropriate means in this context.

---

145 Michael McCarthy, "Experts Warn on Data Security in Health and Fitness Apps" (2013) *BMJ* 347.

146 EDPD, art. 17(1).

147 *Ibid*., art. 16.

148 *Ibid*., art. 17(1).

149 Kuan Hon, "Data Security Developments under the General Data Protection Regulation" (2015) *LexisNexis, World of IP and IT law.*

150 GDPR, art. 25.

151 *Ibid*., art. 32.

Also with companies and third parties that have (lawful) access to the data gathered via QS, there can be situations in which data is processed in a way users did not directly consent to. A revealing example is a situation that occurred in 2012, when the *New York Times* showed that a retail chain had used data mining and processing techniques to predict which female customers were pregnant, even when they had not yet announced publicly that they were pregnant (in fact, some of them were not even yet aware of it).[152] This happened on the basis of information that was linked to the Guest ID of customers, a unique code assigned to every individual shopper. This was linked to information such as credit cards, the use of coupons, surveys that were filled out, website visits via e-mails, demographic information (age, which part of town you live, estimated salary). Furthermore, the supermarket could *buy* data about ethnicity, job history, whether or not a person went to college, political leanings, magazines you read, and many more.[153] When this is combined with research about how habits work, supermarkets can learn to control habits.[154] Based on certain data (which ones exactly is unclear), the supermarket was able to create a list with thousands of women who were most likely to be pregnant.[155] Their aim was to "entice those women or their husbands to visit Target and buy baby-related products".[156] In Europe, the GDPR helps to protect individuals against this type of targeting, since data can only be gathered for a specific purpose, unless there is consent of

---

152 Charles Duhigg, "Psst, You in Aisle 5" [2012] *New York Times*, § 6 (Magazine) available at http://www.nytimes.com/2012/03/04/magazine/reply-all-consumer-behavior.html (accessed 5 December 2017) p. 30.

153 Charles Duhigg, "How Companies Learn Your Secrets" [2012] *New York Times* available at http://www.nytimes.com/2012/02/19/magazine/shopping-habits.html (accessed 5 December 2017).

154 Kate Crawford and Jason Schultz, "Big Data and Due Process: Toward a Framework to Redress Predictive Privacy Harms" (2014) 55(1) *Boston College Law Review* 93-128, p. 98.

155 *Supra* n. 153.

156 *Ibid.*

the individual.[157] However, when the purpose is 'to serve the needs of customers', there does not appear to be any problem with the GDPR, when the goal is specific enough. In this way, the GDPR does not always protect external freedom.

A third problem is that many QS-apps collect information about health. Although data directly related to health are protected under a stricter regime, data about behaviour in general, such as showing interest in certain information, or abilities to run etc, can also reveal a lot of information about one's health.[158] This means that, although the GDPR does aim to protect data concerning health, it may not be enough.[159] The external freedom of individuals can be affected, and the GDPR will not always offer enough protection.[160]

Fourthly, there is the risk that companies, based on an existing set of data, try to predict an individual's future behaviour. This can happen via a predictive model that predicts the possible future data, and thus reacts on not-yet-existing data. This is an external limitation of freedom in its most extreme form. Crawford and Schultz state, "these privacy problems go beyond just increasing the amount and scope of potentially private information. Based on existing publicly available information, Big Data's processes can generate a predictive model of what has a high probability of being [personally identifiable information], essentially imagining an individual's data".[161]

---

157 GDPR, art. 6(4).

158 Nicolas Terry, "Protecting Patient Privacy in the Age of Big Data", (2012) 81(2) *UMKC Law Review* 385-415, p. 394.

159 *Ibid.*

160 See for example: Ari Juels, "Targeted Advertising … and Privacy Too" in David Naccache (ed) *Topics in Cryptology – CT-RSA 2001, Lecture Notes in Computer Sciences* (Berlin: Springer, 2001); Catherine Tucker, "Social Networks, Personalized Advertising, and Privacy Controls" (2014) 51(5) *Journal of Marketing Research* 546 – 562; Hamed Haddadi et al.,"Targeted Advertising on the Handset: Privacy and Security Challenges" in Jörg Müller, Florian Alt and Daniel Michelis (eds) *Pervasive Advertising* (London: Springer-Verlag, 2001) 119-137.

161 *Supra* n. 154, p. 98.

Other problems related to external freedom are not solely applicable to QS. These problems are not fundamentally different when looking at QS, but apply to all data and privacy challenges. First of all, it is questionable whether it is even possible to give consent for the processing of your data, when it is not clear for what purpose this consent is given exactly, as the GDPR asks.[162] Secondly, it is difficult to assess the exact scope of the consent asked for in the GDPR.[163] Thirdly, the protection of personal data in apps (including QS) can be problematic.[164] Here again, the GDPR only asks for 'appropriate measures', without specifying. This might also make it possible to affect external freedom, without the GDPR protecting the individual sufficiently. Moreover, there is a risk that companies combine sets of QS. This is a realistic problem, especially when it is about free QS-tools, since controllers might sell user data to other companies to earn money.[165] Whether or not this is protected by the GDPR depends upon the consent that has been given by the user.

Although processors are obliged to anonymise the data they sell (e.g. through pseudonymisation, encryption or key-coding),[166] this does not make it impossible to identify specific individuals.[167] Thus, anonymisation does not

---

[162] See for an article going in depth on the topic of consent: Daniel Solove, "Privacy Self-Management and the Consent Dilemma" (2013) 126 *Harvard Law Review* 1880-1903.

[163] Eve Caudill, Patrick Murphy, "Consumer Online Privacy: Legal and Ethical Issues" (2000) 19(1) *Journal of Public Policy & Marketing* 7-19.

[164] Simson Garfinkel and Gene Spafford, *Web Security, Privacy, and Commerce* (Sebastopol: O'Reilly Media, 2002).

[165] Cesare Bartolini et al., "Assessing IT Security Standards Against the Upcoming GDPR for Cloud Systems" [2015] Presentation at Grande Region Security and Reliability Day 2015.

[166] Omer Tene and Jules Polonetsky, "Privacy in the Age of Big Data. A Time for Big Decisions" [2012] *Standford Law Review,* available at https://www.stanfordlawreview.org/online/privacy-paradox-privacy-and-big-data/ (accessed 5 December 2017).

[167] Paul Ohm, "Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization" (2010) 57 *UCLA Law Review,* 1701 - 1765; Arvind Narayanan and Vitaly Shmatikov "Robust De-anonymization of Large Sparse Datasets" [2008] *Proceedings of IEEE Symposium on Security & Privacy* 111-125.

necessarily lead to anonymous data. Again, the GDPR might not offer enough protection to ensure that individuals' external freedom is protected when using QS, especially when the sold database does not turn out to be all that anonymous.

## 6 Conclusion

In conclusion, it is not difficult to see that the QS can influence one's freedom and autonomy. Some aspects of the GDPR are positive in this light: the GDPR is also applicable to apps offered outside of Europe, the GDPR contains an obligation to ask for consent before processing data, and specific consent is required for the processing of health-related data. Finally, personal data can only be collected for specific purposes. However, many of the problems regarding external freedom that are mentioned in the article, are not addressed by the GDPR. Much less familiar but at least as problematic as external freedom is the restriction of internal freedom. Although this is really problematic, the GDPR does not touch upon any of these aspects, which makes the GDPR unable to protect internal freedom as influenced by QS. This article adds to the debate on internal freedom. Not much information is available on this topic, beyond the potential uses of the technologies. This in comparison to external freedom that has been explored in a plethora of works in greater depth. More research on the issue of limitations on internal freedom related to new technological developments, such as the ones that underpin QS, is therefore required.